~~TOP SECRET~~

ARMY SECURITY AGENC

DF-176

(7)

[illegible]

Copy No. 37

From: [illegible]

To : ______

Declassified by NSA 08-01-2007
pursuant to E.O. 12958, as
amended, FOIA Case# 9329

~~TOP SECRET~~

DOCID: 3189580

DF-176

~~TOP SECRET~~ 83/49/TOPSEC/AS-14

ANSWERS WRITTEN BY PROFESSOR DOCTOR WOLFGANG FRANZ

TO QUESTIONS OF ASA EUROPE

1. The attached report contains a translation of the answers written in April 1946 by Professor Doctor Wolfgang FRANZ of the Mathematical Seminar, Goethe University, Frankfurt to questions posed by ASA Europe. At that time Dr. FRANZ was living at Schumannstrasse 58, Frankfurt and was visited in his home by Captain Mary C. LANE, then assigned to ASA Europe.

2. Dr. FRANZ, who is mentioned in various TICOM interrogation reports (see among others TICOM/I-1,31,71,94,96,123,124,145,201,202) was Professor of Mathematics at the University of Goettingen when in 1940 he joined OKW/Chi as a member of HUETTENHAIN's section. His main contribution to cryptanalysis was the solution of the United States diplomatic strip system, for which he was given considerable credit by his colleagues. This report describes in general fashion the solution of this system. Of interest also is Dr. FRANZ's estimate of fellow German cryptanalysts, particularly of ROHEN (see also T/I-199), HEIDLAND (see also T/I-202), and FEHNER (see T/I-206), wherein the opinion of TICOM interrogators of these men is independently confirmed.

3. Personal contact with Dr. FRANZ indicated that he was a gentleman of unusual scholarship and integrity, an impression confirmed by the report.

September 1949

Translated: ASA

35 copies: Copy No._____

14 pages
1 appendix

~~TOP SECRET~~

DOCID: 3189580

Written Replies by Dr. Wolfgang FRANZ, Professor, Mathematisches Seminar der Universitaet Frankfurt, 19 May 1946 to Questions of ASA Europe

I. PERSONAL

A. Birth: I was born 4 October 1905 in Magdeburg, the son of a teacher, later Director, Professor Doctor Erich FRANZ, presently in Hamburg, Germany.

B. Marriage: On 11 March 1939 I married Dr. Katharina FRANZ, nee KORN. I have no children.

C. Travel and Education: After graduating from the Reformreal-gymnasium, Kiel at Easter 1924, I devoted myself to scientific study, primarily mathematics, secondarily philosophy, physics, music, and literature. I studied at the following universities:

1924	summer	semester	Kiel	winter semester	Kiel
1925	"	"	Vienna	"	Kiel
1926	"	"	Berlin	"	Kiel
1927	"	"	Kiel	"	Kiel
1928	"	"	Kiel	"	Halle
1929	"	"	Halle	"	Halle

On 26 February 1930 I received the degree Dr. rer. nat. at the University of Halle. Professor HASSE, then at Halle, was the reviewer; my dissertation dealt with HILBERT's Theory of Irreducibility. I have done no travelling except to and from the above-named universities, to scientific meetings within Germany, and occasional vacation trips inside Germany and Austria, and one official journey, described under II b 1 below, during my association with the Armed Forces.

D. Career before the War: After receiving my degree I was at first Assistant at the Mathematical Seminar at the University of Marburg under Professor HASSE, who meanwhile had been called to Marburg. I occupied this position from May 1930 to November 1934. During this time I performed assistant's duties at lectures and practice

DOCID: 3189580

work in scientific labors; I also made certain scientific investigations of my own (see appended list of publications). Because of differences of opinion with Professor HASSE in scientific and primarily in philosophic matters, I did not follow him to Goettingen when he was called there in 1934 but took a position as assistant to Professor REIDEMEISTER in Marburg. Since then my work has been in arithmetical and algebraic investigations in topology. I have also been concerned with the theoretical aspect of logic. From the winter semester 1935/36 to the winter semester 1936/37 I was authorized to hold lectures on applied mathematics at the University of Marburg. On 4 March 1936 I became Dr. phil. habil. with a treatise (Habilitationsschrift) on the Torsion von Ueberdeckungen at the University of Marburg under Professor REIDEMEISTER. Because of financial difficulties I moved in August 1937 to the University of Giessen as Dozent and Assistent, where I remained until the beginning of the war. Even then I was in active contact with Professor THRELFALL in Frankfurt and was seeking to move to Frankfurt. When, after the beginning of the war, the University of Giessen was closed, I spent a semester as substitute at the University of Goettingen. On 17 July 1940 I was ordered by decree of the Kultusministerium to report to Berlin for service with the Cipher Bureau of the Armed Forces (WNV/Chi), as is described in detail under II B below. Meanwhile my instructorship was transferred to Frankfurt (in 1940); at the expiration of the customary six years as instructor, I was appointed in 1943 as Supernumerary Professor at Frankfurt. Since the end of the war I have been in Frankfurt and am lecturing on all fields of pure and applied mathematics. I have made no speeches and issued no publication other than my lectures on mathematics at the universities, institutes, and scientific meetings of the German Mathematical Association

and aside from purely mathematical publications enumerated in the list attached, and talks in my official service with the Cipher Bureau (Chi IV) as mentioned under II B below.

E. Military Career: Because of my distaste for military service and absorption in my scientific calling I never volunteered for military service. I was never a soldier; during the entire war I was classified as "UK" (Unabkoemmlich indispensable). For my service with the Cipher Bureau see under II.

II. CAREER AS CRYPTANALYST

After the outbreak of the war in 1939 I was first classified as UK for the University of Giessen. It soon appeared, however, that early or late I must count on being called for service. Since I had no previous military training and under the circumstances did not look forward with any great pleasure to training as a recruit, and since, on the other hand, the majority of university mathematicians were in course of time being employed in non-military activities with the Armed Forces, I began looking around for some such employment where I could use my mathematical training. Among various possibilities which occurred I took the first best one: a friend and colleague who was working at the Observatory in Babelsberg wrote me that a college friend of his, a certain Mr. HUETTENHAIN, who was working for an important office of the Armed Forces, needed mathematicians. Presumably the work would be half-way interesting, at least in comparison with other possibilities. Was I ready to accept an invitation from this source? I declared myself ready and after a relatively long time on 13 July 1940 received instructions to report immediately in Berlin for service with the Cipher Bureau (OKW/Chi). At the same time I also received from the Kultusministerium, which is the highest authority in university affairs, telegraphic instructions to accept the invitation. I went to Berlin and reported at the office, was received by a Major BRUNSKE who was in charge of personnel matters, and after a considerable number of other

DOCID: 3189580

introductions and charges [illegible] was assigned to Government Counselor (Regierungsrat RR) Dr. HUETTENHAIN, that friend of my colleague. He revealed to me in a general way what the work was. Up to this moment I had never had anything to do with cryptographic affairs, and never even heard of such except in novels or newspaper articles and had no ideas on the subject.

My position at the Bureau was that of a Beordert-en Beamte, i.e., I remained an official of the University of Giessen and drew my pay from there; when, on 1 October 1940, after I had gone to work for the Bureau, I was transferred at my own request to the University of Frankfurt, I was paid by the latter university. However, I received supplemental pay from the Bureau, and also a supplement for ministerial rating. Several times while working for the Bureau I was called up for induction but was released each time; my military pass contains the record of such a call with subsequent release. I did not have a soldier's pay book (Soldbuch) and never wore a uniform.

II B. DETAILS OF ACTIVITY WITH OKW/Chi

I shall now give a chronological report on my work at the Bureau; individual questions not treated here will be answered at the end.

First, I had to solve a number of problems which were intended as aptitude test and instruction. The simplest was a monoalphabetic substitution, then came easy superenciphierments, nulls, polyalphabetic substitution, substitution tables, variants, and transpositions of various kinds. Since I was able to solve these rapidly I was soon given other tasks. I had to investigate a cipher device built by Oberinspektor [illegible]ER for the use of the troops to determine its practicability. It was a cylinder with interchangeable bars which, on the one hand, was complicated, but which was probably not quite secure enough. This work occupied me for some time since at the same time I had to get a basis for judging security demands. Meanwhile, I became a little acquainted with the set-up of the Bureau, at least insofar as HUETTENHAIN's section

was concerned. This section which consisted of RR Dr. [illegible] (at that time he was not yet RR), an assistant Fr. GRASSL, and secretary, had two assignments: (1) to aid, on the theoretical and mathematical side, in difficult problems of cryptanalysis which could not be solved by the philological experts (generally RR) for the individual countries, (2) to test apparatus intended for our own /German/ use. I did not become acquainted with the heads of the different language sections until quite late, most of them not until 1943 or 1944. As my first cryptanalytic-technical assignment I had to assist in the solution of a Mexican cryptographic system. The name of the section head, a quite unimportant employee, escapes me. It was a perfectly simple code which, if I recall rightly, had alternate values which were cyclically displaced and could be solved in a simple manner without mathematical aids. There I found for the first time something which I was to observe again and again, namely, that the work at the Bureau was carried on in an utterly irrational manner and that many of the language experts, even in the more important sections, had not the simplest acquaintance with the field of mathematical cryptanalysis. They confined themselves to solution of plain codes. The immediate superior of Dr. HUETTENHAIN, Ministerial Counsellor FENNER, with whom I became acquainted a few years later, did try, to be sure, to overcome this deficiency by [illegible] courses on the simplest points. But only the lower and younger employees participated in these courses. Later I had a Greek [illegible] to work on. It was a 5-place code where, curiously enough, the middle letter (or middle digit?) designated the grammatical form of the word in question. This code was enciphered with a 2-place substitution table. The solution was tedious but not essentially difficult. After the German troops entered Greece, a complete set of the substitution tables used was captured and I was able to identify some of the tables I had solved, in modified form, of course. In the course of time several other ciphers

DOCID: 3189580

were laid before me, most of which proved insoluble, at least with the volume of traffic at hand.

Especially laborious and difficult work was connected with an American system which, judging by all indications, was of great importance. This was the strip cipher* system of the American diplomatic service which was subsequently solved in part. After I had been working on it a long time and was beginning to get some insight into the system, the work was greatly furthered by some captured material. This was given me with no word as to its provenance. From inscriptions and notes, however, one could infer that these were Japanese photographs. These were the basic material of the so-called "intercommunication strip cipher system O-1" and three further sets for special circuits between the Department and Reval, Tallin and Helsinki (?) with designations of the type 19-1 or something similar. With these, several older messages could be read and the door was opened for further study of the system.

This strip cipher system, when rightly employed, doubtlessly has great advantages. It appears to me, however, that it was not used with sufficient caution. Only through carelessness, in part through lack of care in setting up, was it possible to break into the system as far as we did. Only after the Americans had obviously noticed that many of their messages were being read was the application so modified that although the basic idea was the same the possibilities of breaking in were materially reduced.

Now even a casual glance at the material showed that the study of this system would call for extensive work. Even decrypting when the strips were completely recovered required much time. One or even two or three workers would not have been able to manage it. Moreover, many other cryptograms were coming in and as time went on the systems became more and more complicated. RR Dr. HUSTINNAIN's plan had long been to engage a considerable number of assistants, partly scientifically trained workers,

---

* [Here FRANZ uses the American term. Translator's note]

partly assistants — so-called statisticians or clerks. Of course, all of this should have been done much sooner. If there had early been an adequate organization, I think the successes of the Bureau could have been multiplied. On the basis of gradual successes with the Am 10 —that was the designation of the strip cipher system — Dr. HUETTENHAIN succeeded in securing the appointment of assistants despite vigorous opposition on the part of the administrative offices and the philological sections. They were appointed as scientific helpers one after another: Professor Dr. Wilhelm WEBER, Berlin; Professor Ernst WITT, Hamburg; Professor Dr. Georg AUMANN, Frankfurt; Dr. Alexander AIGNER, Graz; Dr. Oswald TEICHMUELLER, Berlin; Dr. Johann Friedrich SCHULTZE, Berlin. As clerks, soldiers were detailed; women students and other qualified women were hired, so that the section finally grew to some 50 persons and formed a curiously mixed group which was regarded with disdain by the other sections because of its non-military character.

II C . DETAILS OF WORK OF GROUP IV, OKW/CHI

The head of the section was Dr. HUETTENHAIN. In the course of three years, however, he was given so many other duties that he would have been glad to split off the mathematical cryptanalytic work and to have made it a separate section. I had been picked as head of such a section, since I was the most experienced of the mathematicians, but this plan suffered shipwreck because the officers in the Bureau did not think civilians were fit for section heads. As I had no ambition in this direction, I never was named section head. To be sure, about 1944 I was acting head of this section. Actually this was the largest section in Group IV; it must be remembered, however, that most of the members were not really trained statisticians, whereas the other sections had only members of long training or perhaps one or two assistants.

I shall now give a short review of the work on Am 10 and the results achieved, so far as this is possible from memory. This work occupied me

to the end of the war. For traffic of the Department with all Embassies a so-called circular traffic (American designations O-1, O-2,...) was used. Moreover, each individual embassy and legation had a system exclusively for use between it and the Department. In all I observed some 70 different traffics (naturally by no means were all solved; many were rarely used). Each individual circuit used the following basic material: a set of 50 alphabet strips with mixed alphabet and the so-called numerical keys, date and order tables. By means of these last, 30 strips were selected in definite order each day and used for encipherment. Historically this system is known under the name of BAZERIES. Primarily it is important that the encipherer can choose arbitrarily with each series of 30 letters any one of the 25 remaining columns as his cipher text column, while the decipherer must pick out among 25 possible columns the correct one on the basis of its making sense. In working on this system the following tasks presented themselves:

(a) Reconstructing from a compromise, i.e., from a message available in both plain and cipher form of the strips used.

(b) Discovery of such a compromise.

(c) Building up of the 30 strips used to get the full set of 50 strips.

(d) Construction of the numerical keys, in particular recovery of the 40 different orders.

(e) Setting up the strips where numerical keys are known.

(f) Recovery of the strips where no compromise had occurred. Regarding these tasks the following may be said:

(a) is not difficult if the compromise passage is long enough and the text is correct. The task may become very difficult, however, or even uncertain if these conditions are not fulfilled. The methods were so far developed that they yielded the solution or showed that solution was impossible, i.e., that the solution was ambiguous.

DOCID: 3189580

(b) is really no mathematical problem. It calls for exact knowledge of the material, sometimes also for a knowledge of other circuits and systems than Am 10; with careful logging and close observation some of the inevitable compromises keep turning up.

(c) is successful according to the amount of traffic available. Repetitions are important; stereotyped beginnings and a fine feeling for the cryptographic habits of the sending stations are also important.

(d) depends entirely upon the material. Sometimes it is not completely successful. For instance, if no material is at hand for individual dates.

(f) is the most difficult and mathematically the most interesting problem. After extensive studies and test cases I worked out such a solution with very good prospects of success, but then by a combination of methods (a) to (e) was able to go ahead faster. In the Foreign Office (f) was also carried through successfully but only after more than a year of tedious effort on the part of a large number of workers.

All told, some 28 circuits were solved at the Bureau under my guidance, likewise six numerical keys — some of them only in part. To be sure, only a few solutions came in good time; in most cases there were lags of one to one and one-half years. Since the essential principles were recognized too late and necessary personnel and aids were not available at the tim

IV D. DESCRIPTION OF MECHANICAL AIDS TO CRYPTANALYSIS

In the way of machine aids we used primarily Hollerith punch machines. Their construction is well known, as they are generally used for statistical studies of all sorts. In addition, there was built at my suggestion at the Bureau an electric machine which permits determining a number of repetitions of letters in a polyalphabetic substitution on a width of 30 with a depth of 20 to 80 lines, taking one line at a time, which naturally is fundamental

for problem (f) above. I cannot give technical details of this machine; its construction and use were in the hands of the section of Dipl. Ing. ROTHSCHILD and his associate, especially Baurat JENKEN. It employed a large number of relays; the polyalphabetic substitutions could be set up with 30 x 25 plug sockets with special weighting figures. In any event, no special principles were involved in this machine and it did not function very dependably. The same difficulty was also met in other machines built or projected for mathematical analysis. They did not function exactly enough; construction took too long. That is the main reason why later we worked primarily with Hollerith machines.

III. RELATIONS TO FINNISH CRYPTOBUREAU

The Bureau maintained regular liaison with the Finnish Cipher Bureau. Each week a courier went there; the head was apparently a Lieutenant Colonel HALLAVA (or some similar name). Once I was sent as substitute to carry the documents with the secondary purpose of allowing me a few days vacation and I spent three days in Finland (16 November 1943). I was supposed to meet Lt. Col. HALLAVA, but he was not there and was introduced to me only on my return journey in Helsinki. He was so lit up that we could not discuss cryptography at all. The Finnish Bureau worked diligently with a small group of members but without any very great results as we could see by the reports which came in.

IV. REMARKS ON OTHER CRYPTANALYTIC WORK AT OKW/CHI

Aside from work on the Am 10 I later helped with a Turkish system or rather advanced the solution which was already well started. It was a relatively simple code enciphered with a 20-letter additive and offered no mathematical difficulties. Its current exploitation could be considerably furthered, however, by appropriate statistical arrangements. I never worked on English ciphers. The successes of the Bureau with these seemed to

DOCID: 3189580

have been slight.

Only in the last years of the war did I get any considerable insight into the work of the other mathematical cryptanalysts. At this time, however, the work was rendered far more difficult by the air attacks on Berlin and the resulting displacements. The most successful work along with that on the Am 10 was that of Professor LITT, who very skillfully solved a cipher of the Polish Government-in-Exile in London. This was a large complicated grille which was laid over a large number sheet. Several such grilles were constructed and messages were read currently. Photographic aids were used in the process. Dr. SCHULTZE worked without special skill and without success on a Swedish machine. Professor LIBER had good initial success with a Japanese system, a reenciphered transposition. Later, however, he could not follow the development; I know no details of his methods.

Toward the end of the war the work became less and less pleasant, not only because of disturbances due to air attacks, but also to the falling apart of various fields of he work because of rivalries and jealousies. I frequently gave talks before the heads of the language sections on Am 10; other mathematicians talked on their work. On the whole, however, this found little echo. The men to whom we talked either met us with distrust or did not want any help from us. At the end of the war I was on an official journey to retrieve some material which had been lent to the Foreign Office, and was overtaken by American troops in northern Germany.

V. ANSWERS TO MISCELLANEOUS QUESTIONS

Head of OKW/Chi: No head of the Bureau after the middle of 1940 was named HOFFNER (the name mentioned in the question). Rather Lieutenant Colonel KETTF, later Colonel KETTLER, was head. There were no others. If I am not mistaken I once heard the name HOFFNER mentioned when they were talking about KETTF's successor. However, I may be mistaken for I never had any interest in questions of officer personnel at the Bureau or in any other unit.

DOCID: 3189580

my superior after HUETTENHAIN, had an excellent reputation as cryptanalyst but in my day he rarely did any of the work himself. In the course of time he had been more and more openly pushed aside by his superiors, in particular by Colonel KETTLER (who was generally recognized as an incompetent and unsuitable head for OKW/Chi) and had become more and more retiring. It was my impression that, if allowed to make his own decisions, he could have built up a cipher bureau which would have functioned incomparably better. Professor NOVOTNY of the Russian language section likewise had insight into the deeper relations but seemed to me to be too old and not active enough. Of the section heads at OKW/Chi those whom I have mentioned and Ministerialrat WENDTLAND, of whom I have yet to speak, were the only ones -- and this is merely my personal opinion -- who could properly be called cryptanalysts.

Ministerialrat WENDTLAND: Ministerialrat WENDTLAND became head of Group V in the very last period of the war; up to then he was section head for the Balkan languages. He was very capable in his work and towered far above his colleagues in ability and character. His efforts to raise the level of the work in those final days, however, were doomed to remain without success in view of external circumstances and the opposition of his colleagues and superiors who were accustomed to the old way of doing things.

Oberregierungsrat ROHEN: The section England-America was under the direction of Oberregierungsrat ROHEN, with three other Regierungsräte, including SCHULZ. It is probably safe to say that ROHEN was not equal to his task from either a technical or an organizational point of view. I assume that he was a good code worker; beyond that I never heard a technically accurate remark from him although his section received the benefit of my labors. His subordinates did as they pleased. Regierungsrat ROTTER did not belong to this section. The various systems, whether solved or unsolved, were numbered Am 1, Am 2 etc. I can say little regarding the character of the individual systems and the degree to which they were broken. Some simple

codes were solved; a substitution table was solved currently or almost currently by SCHULZ who was the most competent of the group. The content of these messages, however, was insignificant. Attempts to gain cribs from them for Am 10 failed. I still recall system Am 9, which occasionally occurred mixed with Am 10 and could be recognized by the two initial letters of each 5-letter group, of which at least one had to be a vowel. It was probably solved to all intents and purposes.

Doctor PIETSCH: Doctor PIETSCH was a mathematician and was introduced to me at a mathematical meeting which had nothing to do with our service. So far as I know, he was Assistant at the University of Berlin. Later he turned up once at a lecture I was giving for section heads (see above). I think he belonged to the Air Force.

German Security Studies: In 1942 I had absolutely no overall picture of the cryptographic work at the Bureau. Hence, I cannot say anything positive in this regard. Naturally there was a general tendency to seek permanent improvement of our own cryptosystems, since it was recognized that many systems regarded as unbreakable could nevertheless be solved if serious efforts were made. In this regard, General GEHLER later made statements of this nature; he was in no wise a technical expert in the subject, but nevertheless was successor to General THILO.

DOCID: 3189580

The following is a list of the publications of Professor Doctor Wolfgang FRANZ, Dr. rer. nat., Dr. phil. habil. as of May 1946.

Untersuchungen zum Hilbertschen Irreduzibilitaetssatz. Dissertation. Math. Zeitschr. 33 (1931).

Zur vorstehenden Arbeit von A. Korselt. Journ. f.d. reine u. angew. Math. 166 (1931).

Aufgabe 89 (Loesung). Gemeinsam mit H. Hasse. Jahresber. d. deutsch. Math. Verein. 41 (1932).

Helmut Hasse, Klassenkoerpertheorie. Ausarbeitung einer Vorlesung von S.S. 1932 und eines Teiles der Fortsetzung von W.S. 1932/1933 an der Universitaet Marburg. Von Wolfgang Franz unter Mitwirkung von L. Elsner und W. Kirsten. Marburg 1933 (autogr.)

Elementarteilertheorie in algebraischen Zahlkoepern. Journ. f.d. reine u. angew. Math 171 (1934).

Die Teilwerte der Ueberschen Tau-Funktion. Journ. f.d. reine u. angew. Math. 173 (1935).

Ueberdeckungen topologischer Komplexe mit hyperkomplexen Systemen. Journ. f.d. reine u. angew. Math 173 (1935).

Ueber die Torsion einer Ueberdeckung. Journ. f.d. reine u. angew. Math. 173 (1935).

Ueber die Torsion einer Mannigfaltigkeit. Jahresber. d. deutsch. Math.-Vereinig. 46 (1936).

Torsionsideale, Torsionsklassen und Torsion. Journ. f.d. reine u. angew. Math. 176 (1936).

Ueber das Dualitaetsprinzip fuer Homologie - Homotopieketten (Vortragsbericht). Jahresber. d. deutsch. Math.- Vereinig. 49 (1939).

Abbildungsklassen und Fixpunktklassen dreidimensionaler Linsenraeume. Journ. f.d. reine u. angew. Math. 182 (1943)